CHAPTER 2

Critical Infrastructure Protection Strategies: The Effect

Introduction

Professor Bert B. Tussing

Professor of National Security Issues
Center for Strategic Leadership
U.S. Army War College

We led off this event with an assessment of where the Federal government is trying to go with Critical Infrastructure Protection (CIP). This chapter will focus on the effects of those strategies. Three different organizations will review, at their level, the costs and the impact on operations of the strategy and intent as it has been laid out in the various strategy and policy documents issued by the Federal government. The organizations represent three different viewpoints. From the interagency, Mr. William Bryan of the Office of the Assistant Secretary of Defense for Homeland Defense, will discuss the "View from the Pentagon." From the State level, Mr. Donald Keldsen of the Maryland Emergency Management Agency will look at "Executing the National Vision from State and Local Government." Finally, Mr. William Ennis of the Defense Industrial Analysis Center will describe "Partnering in Defense Industrial Base Protection.


Prudens
Futuri

The View from the Pentagon

William Bryan

Director for Critical Infrastructure Protection
Office of the Assistant Secretary of Defense
for Homeland Defense

Let's begin with a fundamental understanding: criticality is time and situation dependent. We can never be sure what assets will be critical.

Our program is evolving and changing. We have been in the CIP business since the late 1980s; we have been in the Defense Industrial Base (DIB) business since the Defense Production Act of the 1970s, when we really started to look at DIB to ensure that we had the commodities and services necessary to support the DoD mission. We have been doing this for a long time, which is good; but it also has made us very slow to shift gears. We have built a very good program with a lot of capability, based, throughout history, on different levels of resourcing. Sometimes we have had a lot, sometimes we have been lean, and sometimes we have been leaner. However, since the Department of Homeland Security (DHS) stood up and, more specifically, since January of this year, we have been involved in producing an Integrated Risk Management Strategy for CIP, an Integrated Risk Management Strategy for the DIB, a Sector-Specific Plan for the DIB (which feeds into the National Infrastructure Protection Plan), and a Plan for Protecting Physical and Cyber Infrastructure—not to mention new DoD Directive 3020, which also deals with the protection of critical infrastructure. The problem with doing all of that is, when the fire is one foot in front of your face, you never have time to sit back and consider the whole problem.

Now that we have developed these strategies—which are built on good programs and relevant activities, but which we had to develop very quickly—where do we go from here? Our new requirements will require new responses that will, in turn, require a major change of mindset for many of us. The problem is too much process and not enough CIP. We need to get out there and start protecting. I have always viewed CIP with a little 'p.' Protection is just one of many mitigation options, and there is no possible way that we can protect everything that needs to

be protected. Force Protection, on the other hand, is protection with a capitol 'P.' In the same way, Infrastructure protection is a capitol 'P' for DHS; it is their mission. However, within DoD we have always viewed infrastructure protection as an "all-hazards" threat. That has been our historic viewpoint, and we still have to take "all-hazards" into account, but we need to step back now, look at all of the new guidance, and develop new approaches to deal with the evolving threat.

There are several issues to be addressed. First, we have to look at the differences between terrorism and all-hazards. For example, PDD-63 was global in nature, but HSPD-7, which superseded PDD-63, is focused primarily on the continental United States. Likewise, PDD-63 is primarily "all-hazards," while HSPD-7 deals mostly with terrorism. Therefore, the system that we had built to meet the requirements of PDD-63 is "all-hazards"-based and global. We do, still, have responsibility for global CIP; but, quite frankly, we are not where we need to be on global CIP because the way we gather information on overseas CIP is vastly different from gathering information on CIP in the United States. We cannot rely on the intelligence community, because they are looking at the "other side," not at the countries where our troops are based or forward deployed. It takes a lot of creativity to get the kind of information we need from host nations to conduct the kind of analysis we need to support our mission.

Our approach is very simple; we ask ourselves three questions. What is critical? Is it vulnerable? What can be done to reduce the risk? Up to this point, that is what has been driving our program. It concerns me, to some degree, when I see people running around all over the country doing assessments who do not really know why they are assessing what they are assessing or tracking the vulnerabilities that their assessments reveal. It has been our approach to try to develop a methodology to first determine what is critical. As I said at the outset, criticality is time and situation dependent. We have a much easier task in DoD because we have OPLANs, we have missions. Therefore, we already know something about the time and the situations for which we must be prepared. We have combatant commanders that can define their mission, and we can take that mission, dissect it, and identify the critical infrastructure assets that we must protect to assure that mission. We can draw a connection all the way from mission execution to infrastructure protection, and that has been our approach. Have we done that for 100 percent of our missions?

No, but we are working on it diligently. We are developing tools that will make the process easier. We are working on self-assessment tools that will help us choose, from among the thousands upon thousands of assets that we have to consider, the few truly key nodes that we must protect. Those then are the assets where we want to put boots on the ground to do vulnerability assessments, and when we assess them, we have to assess them not only from the "all-hazards" perspectives, but from the viewpoint of this new threat. We are still not doing this well. We have the Cold War methodology, which worked, which still works, and which is still necessary, but which is not enough to deal with the terrorism threat—a hazard that thinks. We have not done as well as we must to develop that methodology. If we get information that terrorists are targeting a specific asset, all we can say is "well, it is not a single point of failure." Not good enough.

Secondly, is it vulnerable? Once we identify those assets that are truly critical, we have to again put boots on the ground to assess vulnerability. We are trying to make this process more efficient as well, and we are looking at a new, modular approach to doing vulnerability assessments for CIP.

Finally, what can be done to lower the risk? In my view, protection is but one of many mitigation options. However, it is a major priority, and it is a tough challenge because it is a shared responsibility, shared between Federal agencies, shared between Federal, State, and local government, and shared between the public and private sector. There are other mitigation options. Sometimes changing procedures can reduce or remove the vulnerability. Sometimes building in redundancy can. We may already have that baseline. That is the way we did business in the past; but we should be concerned that it may not address the complete threat picture.

One of our challenges, then, is determining how we will build on our baseline. What kinds of new skill sets do we need to develop? What new relationships and partnerships do we need to form? How do we improve our information sharing process? These and many other issues must be addressed as our concept of critical infrastructure protection evolves. I have always looked at CIP as a risk management approach. Our intent is to try to minimize the number of critical assets that could be a target. We

know we cannot protect them all, but we must do what we can to reduce the number that must be protected.

We are working more and more closely with the intelligence community, particularly at DHS. We are developing a more effective relationship with the Information Analysis folks at IA/IP. However, it has been very difficult. We have a capability that is science and engineering-based. Meanwhile, the intelligence community has an intelligence analysis capability, and nowhere is that science and engineering capability integrated with that intelligence analytical capability. An intelligence analyst does not think like a scientist or an engineer, and vice versa. We need the intelligence analyst asking the right kinds of questions to get those scientists and engineers looking in the right places. We are trying to build that kind of a program right now.

In regard to information sharing, which is different from intelligence, we do have a system called the Homeland Defense Mission Assurance Portal that we are currently sharing with the Transportation Security Agency and others. This portal is a geospatial information and services (GI&S) environment in which we have over three hundred homeland defense databases that can be overlaid one on top of one another. We have a responsibility to share the tools, processes, and methods that we are using in DoD. We are currently providing that capability to DHS, and our intent is to provide it to all of the States via the National Guard. Unfortunately, it is currently restricted to the SIPRNET, but I have challenged our people to make that same capability available in an unclassified environment so that the information is available to our State and local first responders.

In closing, I would suggest that our next step will be applying our current capability to the twenty-first century. How do we move from looking at the issue from an "all-hazards" perspective to determining how best to disrupt the planning of a terrorist attack against our infrastructure—especially in the case where we know many specifics of where that attack is going to occur.

Executing the National Vision from State and Local Government

Donald Keldsen

Urban Area Coordinator
Maryland Emergency Management Agency

This presentation is intended to provide some perspectives on CIP from the State and local viewpoint. I specifically want to point out some of the effects of implementing CIP strategies at the State and local level. There are four primary effects: confusion, frustration, manpower expense, and little tangible return on efforts.

We all know that CIP is complicated and difficult, and we—all of us—have made some marked improvements over the last three years. We also all recognize that we still have a long way to go.

As CIP has evolved over the last seven years, several points have become evident. One of the first points was that the National Guard had a program, but one directed from DoD. This program began as key asset protection, focusing on the DIB. It was modified into a critical asset assurance program, which focused on a business-continuity approach as applied to the DIB. The confusion results because, while the National Guard may understand that approach, the rest of State government hears that the National Guard has a program to protect "critical assets," and they think that the job is already done. It is not already done. The National Guard's program is focused on the DoD mission as the Lead Federal Agency for DIB protection—not on the other twelve key sectors, not on all four key asset areas.

The frustration arises because there is simply not enough manpower available at the State government level to understand and manage all that CIP implies. State government and local government are very lean. As an example, my spectrum as an Urban Area Security Initiative Coordinator covers awareness, preparedness, prevention, protection, response, and recovery. I cannot just focus on CIP. Even within the National Guard, CIP has always been a kind of additional duty; they did not really have the resources to dedicate solely to the CIP mission. As a result, at the

State level, the response has been, "we are not sure what this CIP thing really means or how to go about doing it." I should say, however, that the expertise of our National Guard personnel, who did understand their portion of the mission, has provided us with a good baseline.

Turning now to assessments—threat assessments and vulnerability assessments—I believe that these are where the programs have to start. The first thing the States had to deal with was the Office of Domestic Preparedness (ODP) threat and vulnerability assessments. They were also required to do capability assessments, but those had more to do with preparedness and the ability to respond. We ended up going through three iterations of these assessments.

The first iteration was back in 2000; we were focused on developing target lists, by jurisdiction, based on threat elements, value of the target to us or to the terrorists, visibility, hazardous materials on site, site population, security, and so on. This assessment was done basically as a train-the-trainer effort by ODP, on a regional basis. Five or six States would get together to be trained on the assessment process, and the States, in turn, would then go out and train the locals. It took a multidisciplinary approach—public health, fire and emergency services, law enforcement, public works, transportation, and others. That effort had several effects. There was confusion over degrees of vulnerability; we had a jurisdiction whose number one piece of critical infrastructure was the Super-Walmart—its rating was the same as that given by Baltimore to the Inner Harbor, a major tourist attraction in the heart of downtown. Obviously, the training and guidance did not result in a consistent approach to measuring vulnerability. Frustration resulted from resistance by the local governments, which have even fewer people to assign to the task than does the State. Additionally, they are resistant to having someone question the importance of their local infrastructure, primarily because their local infrastructure is inherently linked to their local economy and their local tax base. As to manpower, there was a lot of work that went into those assessments, and we never really saw any significant follow-up to the assessment process. Certainly there was some money for equipment and training applied to the first responders, but we saw little follow-up directly related to CIP.

In the second iteration of this same assessment, in the National Capitol Region, ODP said that they would do the training themselves. The implication we took from that was that we had screwed up the first time, but now ODP was going to straighten us out. That did not work any better. Additionally, ODP was going to provide us a summary and analysis of the information—we are still waiting.

Confusion once again had to do with establishing norms. We had a rural county that evaluated the threat to their infrastructure to be at the same level as the threat that the District of Columbia assessed to their infrastructure. Here we had vastly different threats, but the system did not differentiate between those jurisdictions. The frustration came, first, from having to do the assessments for a second time; and then, from what people saw in the lack of common definitions and the resulting confusion. The lack of feedback also caused frustration. We had an automated system that was supposed to provide analysis of the information in order to help us develop our strategic plan; however, we ended up having to hire a consultant to hand grind the information so we could use it. Once again, there was little follow-up from the CIP perspective. The focus of the funding that was generated from these assessments was for preparedness, response, and recovery capability—not CIP.

We were offered a third opportunity, a chance to revalidate the assessment. We [in Maryland] did not sign up.

At the State level we have done some things simply because we saw the need. We assigned State departments and agencies to focus on sectors based on the reporting requirements for dealing with Y2K, and that worked out very well. Since then, our efforts to get State departments and agencies involved with their private sector counterparts for dealing with CIP has had very limited success. There is no mandate or requirement to do this, so we get very little buy-in for the process.

Some jurisdictions are trying to develop local-level initiatives. One county brings in all of their key private sector partners for one day, once a year, to address CIP. Unfortunately, as it turns out, each entity only has about five minutes to express its concerns, so this ends up being a very superficial approach. Still, that is a start.

Another program comes from yet another Federal partner, the Department of Justice, which has tasked the Joint Terrorism Task Forces

(JTTF) to get involved in CIP. In our case, the Baltimore JTTF is truly an integrated Federal, State, and local entity. Cooperation is wonderful; it really works well. In fact, there is a Maryland State Police lieutenant who is in charge of the squad in the JTTF that is responsible for CIP. The mission of that squad is primarily an intelligence effort conducted through outreach programs. For example, they are working with dive shops so that, if there is a suspicious interest in some particular underwater activity or capability, those shops know to call in and report it. Out of the three thousand or so organizations they routinely deal with, probably one thousand have a critical infrastructure focus as opposed to an intelligence focus. However, this creates some confusion, because the State people see this and think, "Okay, they are taking care of CIP;" but, just as with the National Guard, this does not cover the entire spectrum of CIP. From a manpower standpoint, we have made the commitment on the intelligence-gathering side because we saw the need. We do get some tangential benefit for our investment, but we still do not have people dedicated to CIP.

The latest program comes to us from DHS. We had an orange alert in 2002, and IP [the Assistant Secretariat for Infrastructure Protection in the Department of Homeland Security's Information Analysis and Infrastructure Protection directorate] gave us—gave the State of Maryland—a list of the sites that we needed to protect. Confusion resulted because we had no idea where the list came from. One site was a defunct chemical plant, no longer in operation. Frustration: Why didn't DHS coordinate this list with the State of Maryland? As to manpower, the State was in a serious bind. Without more specific, credible threat information, we had no idea how much protection was required. We were operating, basically, in a vacuum. As to resources, one mayor in Maryland will tell you that the Federal government will only reimburse 28 percent of his costs for this kind of protection. In short, State and local officials remain somewhat dubious about the return for their efforts because the threat was unspecified, the assigned sites were questionable, and there was no concept as to how much protection was needed.

Currently, IP has a list of sixty-five sites for the State of Maryland. Sometimes, it is thirty-five. This year, we compared their list and our list; only seven sites were the same. Obviously, we still do not have our terms sufficiently well defined. This is frustrating, and we need to get it right.

Most of us want our goods and services to be cheap, to be good, and to be fast. The reality is that you can only get two out of those three at any one time. You can get it good and fast—but it will not be cheap. You can get it fast and cheap—but it will not be good. You can get it good and cheap—but it will not be fast. The point is, whatever we do, we have to get it good.

Another new program is the Buffer Zone Protection Plan. Initially, this program was focused on nuclear power plants, and the confusion here is that, for us, there is nothing really new with this concern. The frustration arises from the fact that the Federal government was talking directly to the power plants without coordinating with the State and local government. That really angers State and local officials. Manpower was the solution, but funds were not available. The State Police increased their patrolling around these sites, but the Federal government was not paying for it. You may be familiar with the term "unfunded mandate." The States certainly are.

Within the National Capitol Region, in particular, buffer zones end up using State and local space. Let me present this from my local point of view. In the District of Columbia—despite Congress's constant complaints—uncoordinated street closures are a problem, and not a part of the CIP and security solution. Recently, in the National Capitol Region, we met with some of the people from IP to discuss ongoing efforts on how to overcome some of these obstacles and address some of these concerns. The National Capitol Region enjoys a unique relationship with the Federal government and probably has access to more information and more contacts than any other metropolitan region in the country. If the National Capitol Region still has these kinds of issues, then every one else must be really lost.

All of these problems are symptomatic of a bigger problem. Even though every plan and every strategy in existence for CIP says to collaborate with State and local entities, it does not happen very often.

There are some positive aspects. In the 2003 State Homeland Security Grant Program, there actually was a fenced allocation for CIP—for security costs, overtime for orange alerts, and so on. That was really good news. Still, there was some confusion about the language. The documents specified that the program was for those sites with "catastrophic impact."

There was some problem with the exact definition of what would be catastrophic.

I believe that we are beginning to change our focus from a manpower approach to a technology approach. That is very positive. You do not solve CIP with manpower; you have to use technology. It may be a huge investment in technology, but it will pay off over time. We cannot afford the manpower. Obviously, the application of manpower—like the National Guard—is appropriate in situations where you have hard intelligence on the nature of the threat and the target, but we have to think beyond manpower for our long-term approach to the overall challenge of CIP.

More recently, we have seen some good threat-based initiatives. The Urban Area Security Grant is one such initiative in which we focus on metropolitan areas that include a lot of critical infrastructure. That program also provided a category of funding for "immediate needs," which basically gave us carte blanche to spend the money on what we felt we needed to get done. In Baltimore, for example, we used these funds to help us improve or create a number of capabilities: redundant power generation, alternate 911 dispatch, and additional surveillance. In the National Capitol Region, the funds were used to improve communications interoperability.

In closing, let me address some of the issues that continue to concern us in State and local government.

There is a lot of Federal interaction with the private sector. That is good, but at the State and local level there is some difficulty in establishing these relationships. Power grids, pipelines, and transportation networks do not necessarily stop at the State border. As a result, State and local levels get left out of the information flow created by this Federal-private interaction. The ISACs, which are primarily trade associations, also tend to go beyond State borders, and we find ourselves left out of the information and coordination loop there as well.

Interdependency correlations between the various elements and sectors of critical infrastructure are still discussed in general terms; we need the specifics. This is really a consequence management issue, but we need to understand those interdependencies because we are the ones who have to respond and manage those consequences.

We still have a problem with the basic task of identifying sites. The Washington Metropolitan Transit Authority is probably on everybody's list, but we do not need to look at the whole thing. We need to identify the critical nodes—not necessarily the thousands of critical points of failure—that really need to be our focus, and we need the strategies and the methodologies to support that kind of focus.

Coordination at the State level needs to go through the State's homeland security advisor as the single point of contact. Otherwise, the left hand won't know what the right hand is doing at the State level.

Finally, we need to know who is out there to help us. Does DHS have the technical staff to do that? Will DHS define or certify, in some manner, a set of consultants that can help us with these issues?

There is still a fragmented approach, in fact, several approaches, to CIP. The State and local governments need to see a comprehensive integrated plan. The National Infrastructure Protection Plan (NIPP) is trying to meet that need, but what we have seen today really lacks the meat. It is too general, too conceptual. Keep in mind that, while the Federal level is talking at the strategic level, in State and local government, we need to work at the operational and tactical levels. Without clear guidance, concrete methodologies, and predictable resourcing, we can't get there.


Prudens
Futuri

Partnering in Defense Industrial Base Protection

William V. Ennis

Director, Contract Management Agency
Industrial Analysis Center

Critical Infrastructure Protection Strategy Effects on the Defense Industrial Base

Protecting critical infrastructure to maintain the private sector's capability to ensure the orderly functioning of the economy and the delivery of essential services is an important element of the National Strategy. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* identifies a clear set of national goals and objectives that underpin efforts to secure the infrastructure. As the DoD Defense Industrial Base (DIB) Sector Lead, the Defense Contract Management Agency (DCMA) works collaboratively with the Assistant Secretary of Defense for Homeland Defense (ASD [HD]), the Defense Program Office for Mission Assurance (DPO-MA), and others actively engaged in DoD strategy and policy initiatives. To date, these initiatives have included the DIB Sector Specific Plan supporting the NIPP, the DoD Integrated Risk Management Strategy (IRMS), and the DIB IRMS.

The National Strategy is complemented by these DoD initiatives. Moreover, the value that DCMA brings to the table is operationally related. There is still a long road ahead to fully deploy a comprehensive program that identifies, assesses, and protects DIB critical assets. Practices and processes need to be institutionalized to assure successful strategy attainment. The following issues will be key elements affecting a timely and effective implementation of processes required to execute the National Strategy as related to the DIB.

Information Sharing and Partnering

In an effort to provide a mechanism for regular interaction with the DIB, DoD is working closely with several industry associations to

develop a Memorandum of Understanding (MOU) outlining a process for identifying issues and working toward their resolutions. The MOU establishes an Action Group to foster a closer working relationship, which will be the foundation for developing a protocol for disseminating and protecting information about critical DIB assets.

The most significant challenge to working with DIB stakeholders is the establishment of legal provisions to support the protection of sensitive information. The DoD requires statutory authority and Department policy that will govern the protection of sensitive information. The Action Group is addressing several specific issues:

- Exemption of proprietary and other unclassified sensitive information from the Freedom of Information Act (FOIA)
- Impact on companies the DoD identifies as owning critical assets
- Liability from inadequate correction of vulnerabilities or for failure to reasonably defend or plan against threat occurrences
- Forced information release as a consequence of "discovery"
- Protection of proprietary or other sensitive information

Additionally, the Action Group must develop specific information sharing policy guidance, processes, and procedures to enhance two-way communication flow between the DoD and the DIB. The DoD and industry have a number of separate and distinct information sources; however, there is little interaction between the two. The DoD and the DIB need to remedy this if there is to be a collaborative effort in protecting the DIB.

Sharing the Burden of Remediation

If DoD identifies significant vulnerabilities that affect a critical DIB asset, DoD plans to work with DIB asset owners to develop alternative courses of action to mitigate or remediate the vulnerability. The DoD and the asset owners and operators will select a particular course of action based on the nature and immediacy of a threat, practical concerns, and affordability. They will share in the decision to implement a remedy. The DoD and DIB asset owners and operators have not yet determined

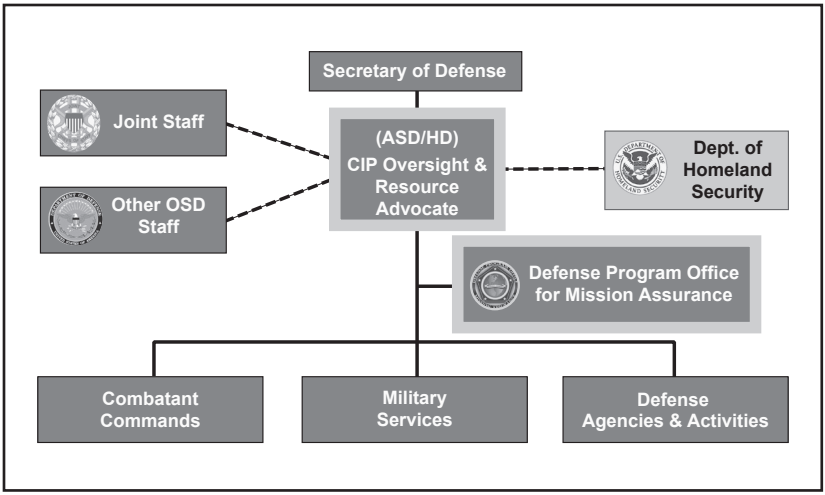

Figure 1: DoD's Organizational Structure for Critical Infrastructure

what will govern how they allocate the financial and operational burden of the selected remedy.

Maintaining Dialogue among DIB Stakeholders

Success depends mostly on the DoD's leadership and collaboration among DoD critical infrastructure stakeholders. The organizational relationship of these stakeholders is illustrated in figure 1.

There are four overall objectives:

- Create the essential formal and informal relationships among DoD critical infrastructure stakeholders to 1) thoughtfully consider diverse proposals for program content, 2) exchange appropriate information about infrastructure reliability and to deal effectively with infrastructure degradation and outage incidents, 3) identify critical cyber and physical infrastructure nodes and links, and 4) develop integrated assessment methodologies
- Acquire feedback from collaborative endeavors to ensure that the Defense Critical Infrastructure Program (DCIP) remains responsive to warfighter needs
- Forge strong partnerships across the Department to ensure that ongoing efforts will reinforce the creation of policy,

resources, and oversight mechanisms necessary to support warfighter physical and information infrastructure reliability and availability requirements

- Forge coordinated working partnerships internally and with State and local governments and off-base infrastructure providers to ensure that vulnerabilities are identified, remediated, or mitigated

There are immediate needs to break down organizational barriers and nurture strong strategic alliances at the operational level in order for DoD to attain acceptable program results.

The remainder of this paper addresses some operational initiatives that DCMA has underway to meet protection requirements for the DIB.

Identification and Assessment

DIB Definition and Sector Characterization

The Defense infrastructure is a complex, interdependent, and decentralized network of systems, services, people, and processes. The Defense infrastructure includes private sector and other government functions, crosses organizational and political boundaries, and provides goods and services to meet Defense-wide operational and business requirements. It is composed of assets that provide the operational and technical capabilities that are essential to mobilize, deploy, and sustain military operations during both peacetime and war. DoD must ensure that national and international infrastructure dependencies do not adversely affect the military's ability to fulfill its mission of national defense and global force projection.

The DIB is composed of hundreds of thousands of companies and their subcontractors who perform under contract to DoD, and companies providing incidental materials and services to the aforementioned, in addition to Government-Owned, Contractor-Operated (GOCO) and Government-Owned, Government-Operated (GOGO) capabilities. DIB companies are both domestic and foreign entities, some with operations located in many countries.

The DIB does not include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities

that DoD warfighters and support organizations use to meet their respective operational needs. These commercial providers fall under the responsibility of other defense infrastructure sector leads.

DoD is concerned with two classes of critical DIB assets:

- DoD-owned infrastructures and assets that support the NMS
- Non-DoD infrastructures and assets that support the NMS

DIB owners and operators protect DIB assets from many potentially hostile threats and hazards. However, the DIB has no authority or limited authority to perform law enforcement functions or to take offensive protective action. Critical assets within the DIB are potentially vulnerable to exploitation that could result in DoD mission degradation or failure. That the DIB exists in an open, global environment exacerbates the susceptibility of critical DIB assets to vulnerability exploitation.

The changing composition of the DIB (e.g., resulting from mergers and acquisitions) and the evolving regulations and policy that govern the relationship of the DoD to the DIB necessitates broad-based, continuing, long-term interaction and collaboration with DIB members to assure DIB capability and reliability. This long-term continuing interaction is vital, as the vast majority of critical DIB assets reside in the private sector.

The DIB is made up of industrial base sectors, sub-sectors, systems and commodities that produce weapon system platforms, components, and expendables. Figure 2 summarizes the current industrial base sectors topology.

The DIB topology is transforming to reflect the military doctrine of Effects-Based Operations. To support this transformation effectively, DIB business practices must also be effects-based. Accordingly, the DIB framework is transitioning to five Operational Effects-Based Sectors:

- Battlespace Awareness – the ability of commanders and all force elements to understand the environment in which they operate and the adversaries they face
- Command and Control – the exercise of authority and direction of a commander over forces to accomplish a mission

Sector	Sub-sector
Missile	• Tactical Missile • Torpedo • Strategic Missile
Aircraft	• Fixed Wing • Helicopter • Unmanned Aerial Vehicle
Troop Support	• Soldier Systems • Clothing & Textile • Subsistence/Medical • Smoke Obscurant • NBC Systems
Space	• Launch Vehicle • Satellite
Combat Vehicle	• Tracked Vehicle • Tactical Vehicle

Sector	Sub-sector
Ammunition	• Bombs and Warheads • Cartridges & Fuzes • Explosives
Weapons	• Small • Medium • Large
Information Technology	• C4I • Information Security • Trainers and Simulators • Computer Peripherals
Shipbuilding	• Surface Ship • Subsurface
Electronics	• Electronic Warfare • SONAR • RADAR

Figure 2: Defense Industrial Base Sectors and Sub-sectors

- Force Application – the engagement of adversaries with lethal and non-lethal methods including all battlefield movement and dual-role offensive and defensive combat capabilities in land, sea, air, space, and information domains
- Protection – defense of U.S. forces and territory from harm, including Missile Defense, infrastructure protection, and other capabilities to thwart force application by an adversary
- Focused Logistics – the capability to deploy, redeploy, and sustain forces anywhere in or above the world for sustained, in-theater operations including traditional mobility functions, logistics command and control, medical logistics, training, equipping, feeding, supplying, and maintaining

Future characterizations of critical DIB assets will monitor the industry on this basis of operational effects-based sectors, assess competition and capability issues on a similar basis, and emphasize the

essential functions of warfighting across the operational spectrum of engagement.

Determining DIB Critical Assets and their Dependencies

Since the DIB consists of hundreds of thousands of corporate and government entities, the collection of data on each entity within the DIB infrastructure sector is neither practical nor an effective use of limited resources. To date, DoD's approach has focused on reducing the magnitude of assets to a manageable number through the use of government DIB subject matter expertise.

To make this effort more manageable in the short-term, DoD experts compiled a list of important Defense contractor facilities using the following process:

- Compiled a list of prime contractors and subcontractors from previous Industrial Base Studies;
- Selected facilities from the compiled list of prime and sub-contractors meeting the following criteria:
  - Sole Source,
  - Obsolete/Enabling/Emerging Technology,
  - Long-Lead Time,
  - Lack of Surge Production,
  - Significant Unit Cost Escalation;
- Identified other facilities that met the selection criteria based on knowledge of sectors and commodities;
- Identified critical DIB assets from the initial list of facilities based on the following prioritized selection:
  - Tier 1: Prime or subcontractor single source that could significantly impact warfighter operations due to non-availability of materiel or service,
  - Tier 2: Domestic sole source with essential and unique technology or industrial capability,
  - Tier 3: Prime contractor with essential capabilities that supports numerous programs or industries,

- Tier 4: Single source subcontractor (with a long re-qualification time) that supports numerous programs across the services,
- Tier 5: Essential advanced technology source;

- Reviewed and revalidated the list of potential facilities and nominated additions.

DoD approves the DIB critical asset list which is reviewed and updated on a semiannual basis.

Vulnerability Assessments and Predictive Analysis

Once it identifies a critical DIB asset, DoD must conduct assessments to determine risks and if those critical assets are vulnerable. These assessments consider impact, vulnerability, and threat or hazard, whether from natural disaster, technological failure, human error, criminal activity, or terrorist attack. This approach to dealing with a potentially large number of vulnerability assessments preserves scarce vulnerability assessment resources for assessments of the most important DIB assets.

If DoD identifies significant vulnerabilities that affect a critical DIB asset, DoD will then work with DIB asset owners to develop alternative courses of action to mitigate or remediate the vulnerability. DoD and the asset owners and operators will select a particular course of action based on the nature and immediacy of a threat, practical concerns, and affordability. They will share in the decision to implement a remedy. The DoD and DIB asset owners and operators have not yet determined what will govern how they allocate the financial and operational burden of the selected remedy.

Concurrently, the DoD is developing a set of standards to conduct Full Spectrum Integrated Vulnerability Assessments (FSIVAs). Once fully developed, FSIVAs will apply to Defense critical infrastructure assets, which include DIB assets. The DoD has been consolidating standards and protocols from numerous vulnerability assessment methods that have proven beneficial across the DoD. The FSIVA effort builds on current DoD vulnerability assessment efforts. The DIB will employ FSIVA standards and self-assessments when they become available. As FSIVA standards are developed, they will also provide

the basis for vulnerability self-assessments conducted by asset owners. Self-assessments will support, but not act as a substitute for, scheduled independent FSIVAs. Meanwhile, DoD organizations such as the Office of the Secretary of Defense, the Joint Chiefs of Staff, the Military Services, other defense agencies, and the Combatant Commands will coordinate to perform vulnerability and risk assessments using predictive analysis. The DoD will select assets for assessment on the basis of the results of the impact assessment. Due to the complexity of most assets as well as proprietary considerations, the DoD plans to analyze each asset separately. The following factors will determine when, how, by whom, and to what extent these assessments will occur:

- Process cycle – certain elements of the assessments will associate with the occurrence or planned occurrence of a given cycle in the DCIP process;
- Time – assessment elements will occur at a given point in time and will have continuing activity over time at and between the given points;
- Asset – the nature of the asset will help shape the nature of the assessment elements and their processes and timing;
- Pre-existing processes – other processes used by or applied to the asset may have relevant information that the DoD can incorporate into the assessment;
- Other assessment element results – other assessment results will help determine the scope, intensity, scheduling, follow-up, and need for one or more of the assessment elements;
- Situational – changes in conditions can trigger initiation, delay, or cancellation of an assessment element.

The DoD is developing a scoring methodology for DIB assets against the potential consequences.

In an effort to forecast potential problems, the DoD will further develop and employ the Defense Industrial Base Predictive Analysis System (code named "Red Flag"), which comprises five sophisticated models:

- CIP (Critical Asset list) – determine the impact on military capability attributable to DIB assets;

- Surge Analysis – determine the ability to increase production quickly to meet emerging warfighting requirements;
- Economic Analysis – determine the economic capacity to maintain continuity of product or service flow to the DoD;
- Technology Analysis – determine the technological ability to maintain continuity of product or service flow to the DoD;
- Financial Analysis – determine corporate financial viability linked to product or service flow to the DoD.

The intent of the "Red Flag" indicator model, currently being tested, is to forecast DIB problems early. The DoD is populating the model with business, economic, industrial, technology, and financial viability information. The Department will then analyze, identify, and predict the extent to which specific critical industrial sites are at risk of failing. It will include a communications link that would allow for the timely transfer of information to customers in order to quickly alleviate problems. "Red Flag" indicators will measure economic (capacity utilization, workload), strategic (mergers, acquisitions, buyouts, R&D/ Facility Investment), financial (profit, stock prices), and operations (strikes, layoffs, contract terminations, Base Realignment and Closure [BRAC]) factors.

The DoD will make the "Red Flag" Predictive Analysis model available throughout the DIB community. The model will provide predictive analysis that enables the user community to avert risk, to enhance acquisition, technology, and readiness investment, and to make war operations decisions relative to industrial base requirements.

The DoD will not conduct on-site vulnerability assessments of all DIB sites. Factors such as urgency, severity of the threat, and vulnerabilities, along with achieved and verified levels of protection and assurance will affect the decision to do an on-site assessment. Self-evaluation tools will help screen out critical asset factors warranting or not warranting further action to investigate or assess or otherwise redress worrisome indicators.

Prioritization

The DoD accomplishes identification and prioritization of DIB critical infrastructure assets by analyzing critical infrastructures and

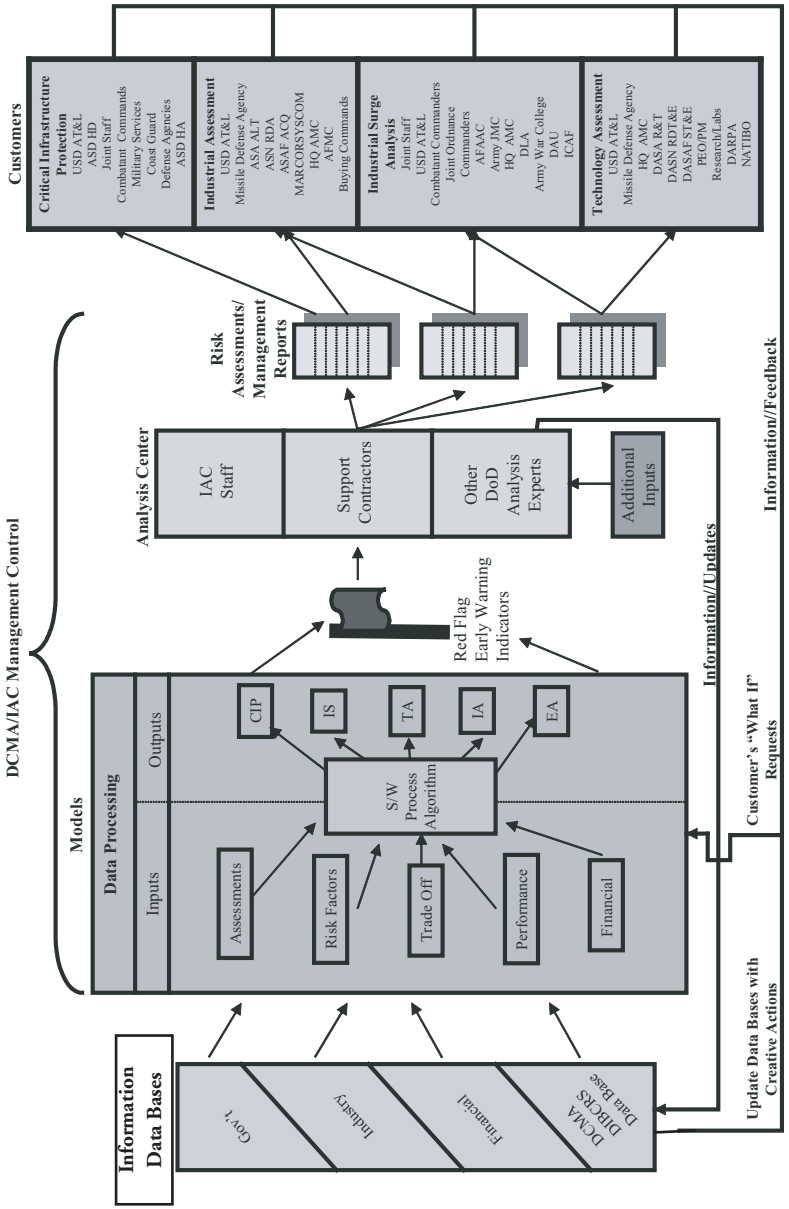

Figure 3: The "Red Flag" indicator model.

their impact on DoD mission achievement. Mission analysis is the key. The purpose of critical infrastructure asset and dependency identification has several elements:

- To identify and prioritize those critical assets tied to each mission requirement, and identify supporting infrastructure assets and their dependence on other assets;
- To determine what assets are critical for mission execution;
- To determine dependencies among assets and dependencies between infrastructures deemed critical to mission execution;
- To determine the impact of the loss or degradation of each critical asset and dependency node on operations.

DCMA's Industrial Analysis Center (IAC) is developing a model for prioritization of DIB assets for both analysis and reduction of risk. The Asset Prioritization Model (APM) is an index model, where the higher the score the higher the risk. The APM scores range from 12 to 151.[1] There are thirteen distinct factors used to calculate the APM score. These factors are broadly classified into Mission Impact, Political, Threat, Economic, and Other.

The overall purpose of the APM is to provide analysts with a quick means to prioritize DIB Critical Assets. The APM is not intended as a substitute for more rigorous assessments such as the Vulnerability Assessment and other assets. Figure 4 shows the thirteen factors used to prioritize the DIB Critical Assets.

Integrated Industrial Capability Risk Assessment Process

To complement the ongoing efforts of identifying and prioritizing Critical Assets and conducting Vulnerability Assessments, the DoD is also performing Integrated Industrial Capability Risk Assessments. These consist of industrial, technological, and financial assessments that can either be fully integrated into the Integrated Industrial Assessment Process, or they can be separate stand alone assessments. The assessments analyze capabilities, technologies, and financial data to identify problem areas and develop resolution alternatives in order to ensure capabilities meet current and future national security requirements. Risk level

[1] Most scores will likely be below 100 unless a contractor employs the majority of the workforce in a given MSA.

Model Factor	Weighting Factor	Factor Classification
Impact Current Warfighting Capabilities	14	Mission
Impact Projected Warfighting Capabilities (e.g.OPLAN 5020)	13	Mission
Impact Multiple Programs	12	Political
Dependency/Interdependency	11	Mission
Recovery Plan	10	Mission
Reconstitution	9	Economic
Corporate Financial Risk	8	Economic
Site Economic Viability Assessment Metric (EVAM)	7	Economic
Threat	6	Threat
Chem/Bio/Rad/Nuclear/Explosive Collateral Damage	5	Threat
Populated Area	4	Threat
Employment Impact - Site Employment as % of State or MSA	3	Economic
Political and Secondary Effects	2	Political
VA Completed/Scheduled	1	Other

Figure 4: Weighted factors used to calculate scores for the Asset Prioritization Model (APM)

ratings are determined based on criteria for each of the assessments. Unacceptable risk may result in the development of intervention actions (remediation).

The Industrial Capability Assessment identifies the essential skills, processes, facilities and equipment, and technologies required to design, produce, upgrade, and maintain the end item and/or key subcomponents. Essential capabilities are defined as those that are integral to the design, production, upgrade, and maintenance of an item and are not necessarily common within industry, are not easily transferable, or are relatively specialized.

The Technology Assessment determines if the technology is unique, essential, or otherwise, and it addresses the state of the technology (emerging, current, or obsolete), whether it is dual use and/or enabling, and how the technology compares to other similar technology based on performance, substitutability, technological superiority, and regeneration.

The Financial Assessment measures the financial capability and viability of a company or operation division.

Remediation versus Protection

There are four levels of DIB Critical Asset Protection Responsibilities:

- First level of protection – Asset owners are responsible for the first level of protection; they have an inherent responsibility to protect their own assets;
- Second level of protection – When asset owners determine they are unable to protect their assets effectively, they should call upon first responders (local law enforcement or emergency services providers) for assistance;
- Third level of protection – When first responders determine that their capability requires augmentation, they should call upon Federal law enforcement and/or State authorities to increase protection;
- Fourth level of protection – In the most serious situations, a State governor may request Federal support or assistance, including military support or assistance.

Shift from Physical/Operational Infrastructure Centric Protection to Remediation Concept

Asset protection efforts, regardless of the level, normally include the use of physical collaboration when it comes to providing infrastructure security. DoD resources cannot support the physical protection of every critical asset. The shift in focus is changing from a physical/operational infrastructure-centric approach to a remediation concept. The first step to accomplish this change is to create redundancy of the capability and capacity of the critical assets. The objective is to ensure that the concept of protection is not limited to physical and operational efforts

solely. Recently, DoD performed a Thermal Battery Study to determine the financial and technical state-of-health for the manufacturers of three types of batteries used in guided weapons. One outcome of the study was to support the expansion of the thermal battery supplier base to include another source, thereby creating redundancy in this critical sub-sector of the industry. This is a prime example of how remediation efforts can provide the Department with an alternative to physical security protection. The creation of additional source(s) will lead to redundancy, thereby reducing the number of critical assets. One determining factor in identifying a critical asset is to determine whether or not that asset is a single or sole source.

Thermal Battery Case Study

Changes in the defense industry have brought about significant challenges to key component suppliers. One of these niche markets is the weapons' battery industry. Some of the challenges facing the weapons' battery industry include consolidation, ownership changes, reduced research and development (R&D) spending, reduced profit margins, and changing government needs and procurement practices. The impact of these changes could adversely affect the DoD's ability to meet its future mission requirements. Industry concerns have been raised about the long term economic viability, lack of R&D investment, and physical plant security.

The DoD currently uses these types of batteries on a wide variety of system applications, including tactical and strategic missiles, smart munitions, and Missile Defense applications, and will continue to do so for the foreseeable future. For the purpose of this study, weapons' batteries are defined as those power sources used in missiles (tactical and strategic) and precision guided munitions (PGMs) and are typically thermal, silver-oxide zinc reserve, and, more recently, liquid lithium (oxyhalide) reserve battery systems.

Thermal batteries are used predominately in tactical missiles and smart bombs. The industry is multinational. The primary suppliers to DoD are Eagle Picher, The Enser Coropration, and Rafael. Eagle Picher furnished 74 percent of the DoD's requirements in FY02. Enser is the main second source for thermal batteries and a unique supplier of lithium cobalt disulfide batteries. These two firms currently produce

approximately 85 percent of the U.S. government thermal batteries (sales). The study concluded that the two U.S.-based businesses, Eagle Picher and Enser, were in an unfavorable financial condition, with both being critically weak. Both firms are highly leveraged, have weak operating margins, and were experiencing net losses. It should be noted that Enser's condition could cause them to possibly exit the market without continued financial support. Eagle Picher has had difficulty servicing their debt, and has other financial red flags. They have tried to improve their position by a complete change of management (45 of 48 executives) and a refinancing of their long-term debt.

The industry in general and Eagle Picher in particular have had difficulties meeting quality and schedule requirements. However, the products delivered have shown excellent performance. Prime contractors and DoD labs are working with these companies to implement corrective programs such as six sigma and lean manufacturing. The thermal battery industry has seen few R&D initiatives being supported either by the government or internally. Most R&D initiatives are for product and manufacturing improvements, with little being done on next generation technology. The thermal battery industry, as a whole, appears to be relatively stable. That's not to say they do not have problems. The industry is presently in an upward cycle as procurement has increased. However, as time moves on and the downward cycles of the past reappear (procurements decrease or less demand due to advances in technology), the problems of the past could become more acute.

The study recommended that the weapons' battery industry and its stakeholders have a problem that requires an overarching domestic strategy. The following was one recommendation suggested to address the thermal battery issue: Determine the desirability of maintaining Enser as a second source for thermal batteries and fund accordingly using Title III or similar funds.

Since the conclusion of the study, two significant decisions have been made by industry and the DoD. Eagle Picher made a corporate decision to expand operations and open a second thermal battery facility in another State. This decision was influenced by a recent assessment that identified potential vulnerabilities. In addition, the U.S. Air Force has made a commitment to increase the capability and capacity of

the thermal battery sub-sector with Title III funding for Enser. This initiative will increase Enser's production capacity to meet future thermal battery demands. These examples are presented as success stories using remediation measures at the industry sector level vice investing in specific physical protection at a single site.


Prudens
Futuri